ELECTRONIC SYSTEM FOR PROTECTION OF VICTIMS OF DOMESTIC VIOLENCE IN AREAS OF INTERIOR AND EXTERIOR

ABSTRACT

This paper presents the results of a research project in which a prototype monitoring and control architecture for victims of gender violence, using mobile technology to determine the location of their potential aggressors previously identified by the penal system develops. Hardware, software and configuration needed to implement a viable technological solution is presented, taking into account the legal constraints, to allow victims of abuse or domestic violence to determine the location of his assailant ensuring that restraining orders meet in public places not covered by the prison system.

Keywords: Electronic control, Location, Bluetooth, Gender Violence.

Darío Fernando Cortés[1]
dfcortest@ucatolica.edu.co

César Orlando Diaz[2]
codiaz@ucatolica.edu.co

Holman Diego Bolivar[3]
hdbolivar@ucatolica.edu.co

1. INTRODUCTION

The denominated “domestic and gender violence” it has been converted in one of the main problems that faces our society. Do not understand frontiers, social classes, cultures, ethnicities or religions. the United Nations agency denominated World Health Organization [1], discloses the principal expression of violence at global scale on its "violence and health" report

The methods of electronic surveillance are alternatives to prison and feature advantages to judicial and penitentiary system because they result less expensive, allows lighten the jails's occupation, besides the guarantee of the human rights fulfillment of those are deprived of freedom and allows the subject remain in its social-work field, does not lose its job, and further, does not suffer the socializing effects of the imprisonment and also can exert on enough control that assures social defence

The 906 law of 2004 on its article 307 stipulates that in Colombia is implemented two types of measures to people sentenced for aggression, custodial freedom and the noncustodial freedom, and within measures of the noncustodial freedom it finds the obligation to subject electronic surveillance mechanisms. The system came into operation in February of 2009, year which had provided the installation of 4.962 surveillance devices, but it's not reached the goal due to the conditions of penal legislation have not allowed. The backwardness in the process is related to specific exigencies provided by the law for beneficiaries. However, the six of February of 2009 was implemented the first electronic surveillance device to domiciliary prisioners

GENSA has been the entity commissioned to total implementation of the system in Colombia, which include the construction of electronic monitoring centers, with related systems for optimal operation, the supply of monitoring equipments, bracelets and all required technologies, among other reasons, by the experience it managed accredit in the construction, for entities of the state, of monitoring centers and telemetry systems [2].

Nowadays the operator and administrator of all technical infrastructure supplied by GENSE is the National Penitentiary Institute with its own staff, through the monitoring centers built and installed by GENSA in cities of Bogotá and Pereira.

The final report of the operations evaluation of the Electronic Surveillance System projects (SVE, for its initials in Spanish) [3], published the three of February of 2012, it recommended, in last, reengineering of the project and also exposed the problems it has been presented, the electronic control system in the legal and technological field. Among the most outstanding are:

Problems in interpretation of normativity:
One of the principal detected problems to the imposition phase of the SVE is the unknowledge and confusion about legal regulation. The researcher

[1] MSc. Electronics, Signal Processing and Communications. University of Seville. Member of the researcher team group TIC201: ACE-Ti. Researcher of Catholic University of Colombia
[2] Doctor of Computer Science, University of Luxembourg. Researcher of Catholic University of Colombia
[3] Doctor en Ingeniería Informática, Universidad Pontificia de Salamanca. Director grupo investigación GISIC Universidad Católica de Colombia

team accessed to multiple and varied judgment elements that allow conclude that an important part of officials, from different hierarchical levels, Involved in the operation of the SVE, ignore in which situations is possible assign SVE and who is competent to do so.

Administrative affairs in the imposition of bracelets:
A variety of problems in the imposition of the bracelets, which correspond to administrative difficulties level, is also identified. These are: absence of criteria for elegibility, little verification of SVE installation conditions, inadequacy of information provided to actual or potential users, lack of Constitutional Court standards regarding payment of fines and insufficient judicial assignments.

Monitoring:
A number of problems had been seen in the monitoring of SVE users that diminish the effectiveness of surveillance that is exerted over persons sentenced of crimes. The GRUVE database indicates that 6% of withdrawals bracelets correspond to leakage of users. Moreover, the Ministry of Justice reports that on December 31 of 2009, identified cases of evasion corresponding to 1,25% of the installed devices, compared to a compliance level of 36% for detention or home detention without EVS. For 2010, the Ministry points out that the percentage of users of VE escapees is 3.6%. What had elapsed in 2011, were evaded 11,8% users. However, these numbers are probably lower than actual levels of leakage, because qualitative research showed a high level of underreporting.

Excess alarms:
One of the larger obstacles that must overcome GRUVE, to effectively monitor devices, is the axcess of alarms. According to the data provided to the research team, between January and May, in 2011, were generated an average of 4.5 million monthly alarms “events”, which means an average of events per minute. There is a contradiction between statics of GENSA and GRUVE about how many of these events are transgressions. According GRUVE, the average monthly alarms transgressions is around on million. Much of these alarms are false as it is the malfunction of devices, momentary unevenness of the base of SVE or users locations at the limits of the perimeter restriction (gardens of residence, for example). Besides, sometimes, alarms can last hours or even days without being checked by an official.

2. PROBLEM STATEMENT AND TECHNICAL RELEVANCE

States must ensure the welfare of the victims, but there are no tools to assure the victim that the aggressor is not near as devices for non-custodial sentences are limited to ensure that the aggressor is at home and also the failures in devices, finding, sometimes, people in malls carrying the device without it has been activated.

This Project proposes a system of monitoring compliance of restraining orders in cases of domestic violence. The practical implementation of the system is seen as two equipments: one for the victim and another for the aggressor. Both systems are based on GSM/GPRS, GPS and Bluetooth/WiFi technologies to locating at any time the victim and the aggressor

The equipment of the victim consists of a handheld device able to alert you to the proximity of the aggressor, while the aggressor equipment consists of a handheld device similar to the victim's appearance and also a bracelet to be kept permanently. The handheld device is responsible for periodically report the position obtained from the GPS system, a control center using GPRS technology. To guarantee that the equipment attacker marks his actual position and prevent a breach of a restraining order the following requirements are established:

- If the abuser tries to get rid of the bracelet, the electronic equipment must reports the incident to the device pocket, in turn, inform the control center.
- If the aggressor and bracelet are separated from the pocket device within a certain distance, this will report the incident to the control center. To determine the distance between elements of the aggressor, an equipment transceivers Radio Frequency (RF) are used in both items.

Some questions arise regarding the limitations on the actions of daily life that may involve the use of the system, in the case of the aggressor. To minimize these limitations, the attacker's machine should fulfill the following:

- ✓ The electronic circuits of the bracelet should have a low energy consumption and, therefore, a sufficient autonomy to require no maintenance for long periods of time.
- ✓ Bracelet must be designed to withstand common situations such as aquatic inmersion.

- ✓ The electronic system of the pocket device should have a low energy consumption and therefore sufficient autonomy as to not require frequently maintenance.
- ✓ The maximum separation distance between the bracelet and pocket device must enable the free movement of the aggressor in small as, for example, a housing spaces, necessarily have to carry the device.

3. METODOLOGY

The structure of the platform can be divided into 2 parts, the first part is focused on the indoor environments such as shopping malls, airports or any different to the home's victim, where will have the central device (hereafter called FARO), the mobile device of the victim and the aggressor's bracelet; in this environment it will make use of the Bluetooth / WiFi technology to the (common to both sides) mobile application to perform calculation of the positioning in relation to the position of the victim and the aggressor. The second part, focused on outdoor environments, count again with the mobile device of the victim and the aggressor handle electronics, but the mobile application will use GPS technology to make the necessary calculations.

Discrimination or differentiation of use of both technologies (Bluetooth / WiFi and GPS) is mainly due to the GPS technology is not very reliable in indoor environments, and this is where comes into play the Bluetooth / WiFi communication, becoming the key differentiator of the platform, and thus ensuring greater reliability and precision.

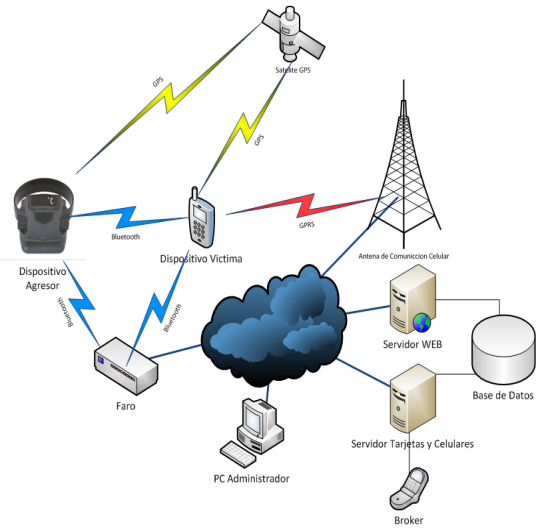

Figure 1. General Scheme system

To explain the internal operation of the system, is taken example in which it is assumed that the aggressor attacks a victim. The perpetrator is prosecuted and found guilty, so proceeds according to the Colombian penal law, and implementing our solution to the problem:

a. The aggressor is assigned a device that cannot be removed from the aggressor and a cell phone with the system software to the victim.
b. The data of the two persons entering the system through a browser by which is accessed the Web page location system. To create individuals and relations must be the system administrator user ID and password.
c. After creating the two individuals, aggressor-victim relationship is established, also the maximum legal distance and is assigned a case manager.
d. At any time it has a record in the database of the last location in any of the two individuals.
e. In case of outdoors environments, aggressor's device sends a message every minute giving his position, which obtained from GPS module of his device. This message reaches the mobile server that is responsible for updating its position in the database.
f. In case of indoor environments, there are 2 possibilities:
- The first is that instead get into the place, a mall for example, but a beacon that scans nearby Bluetooth devices every 20 seconds, because it is the minimum time interval in which scanning is performed unnecessarily have to remove the cache data and send its location using a TCP message to the cell server that also updates its position.
- If the place where the person enter does not have the beacon, the watch alert mechanism would be the Bluetooth that scans devices around and sends through GPRS to the cell server which processes the information

Based on this scheme we can make the definition of the system requirements:

1. The system will continuously search for mobile devices of victims and aggressors.
2. The system must ensure real-time location of both the aggressor and the victim.
3. The system must immediately inform the victim and the management system when victim and aggressor are within a secure space.
4. The beacon will have a copy of the database management system where all devices of victims and aggressors registered in the system relate.

5. The beacon and the device of the victim have redundant GPRS and WiFi communication with the management system to guarantee that there is no loss of communication.
6. The application software of the device of the victim should prevail in its operation over other smartphone applications and cannot be disabled by the user.
7. The system will keep a register of the last location of aggressor's bracelet.
8. The system should allow updating its database and report these updates to existing beacons.

After analyzing the different existing technologies in the market, potential solutions to implement the three devices are:

BEACON	
DEVICE	**FUNCITÓN**
Raspberry Pi	Embedded system technology that will host the communications and control system
WiFi Module	Allows Wireless communications standard IEEE 802.11g
Bluetooth Module	Allows Wireless communications standard IEEE 802.15
RF Module	Allows Wireless communications in the 434 MHz range
GSM/GPRS Module	Allows data transmission on bands of 900MHz, 1800MHZ, 1900MHz

Table 1. Hardware beacon

AGGRESSOR'S DEVICE	
DEVICE	**FUNCTIÓN**
Microcontroller	Performs the tasks of monitoring devices and resource management
Lithium Battery	Assure the battery of the device at least 3 days
Bluetooth Module	Allows Wireless communication IEEE 802.15 standard
RF Module	Allows Wireless communications in the 434 MHz range
GSM/GPRS Module	Allows data transmission on bands of 900MHz, 1800MHZ, 1900MHz

Table 2. Hardware aggressor device

VICTIM'S DEVICE	
DISPOSITIVO	**FUNCIÓN**
Smartphone	Phone with GSM / GPRS, GPS and Bluetooth connectivity that will host the application location. The mobile must be high-end to avoid wrong GPS locations.

Table 3. Hardware victim device

The description of the proposed architecture is the following:

"In the place that will want to implement the surveillance system a beacon will be installed, embedded system based on microcontroller which will have connectivity GPS, GPRS, WiFi, RF and Bluetooth and whose function is to make a permanent monitoring of the place in search of devices of victims and aggressors assigned bracelets. This beacon has wireless communication standards needed to ensure that it can locate these devices when the GPS cease to be reliable for being in a closed environment.

The victim of aggression has a smartphone that has GPS connectivity for outdoor location and Bluetooth standard. The beacon constantly searching for Bluetooth devices and when it locates the smartphone sends notification of the situation to the victim and the central management system, while searching for aggressor's bracelet related with that victim to verify whether it is in the same place or not.

The aggressor is assigned a monitoring bracelet anchored in his forearm which also features GPS, GPRS, Bluetooth and RF standards that can be identified by the beacon as soon as the aggressor entering the place. Once identified, the beacon searches its database device related with the victim and tries to locate it in the place to notify the victim and control system.

4. BACKGROUND

4.1 GPS

The Global Positioning System (GPS) is a system for determining the position of an object (person, vehicle) with a precision of a few meters around the world. The system was developed, installed and used by the United States Department of Defense. To determine the positions on the globe the GPS system consists of 24 satellites and uses trilateration.

The GPS system has an Operational Control Segment, which consists of the central control station (Master Control Station) located in Colorado (United States), three supervisors and a terrestrial antenna stations. Each of the ground stations has highly precise coordinates and are scattered in length with a regular shape. These stations receive signals from all satellites.

With the data obtained from the Central Station, a forecasting of the behavior of oscillators is made and determines the parameters contained in the navigation message, these are sent by ground antennas and from there to satellites in the band S [4].

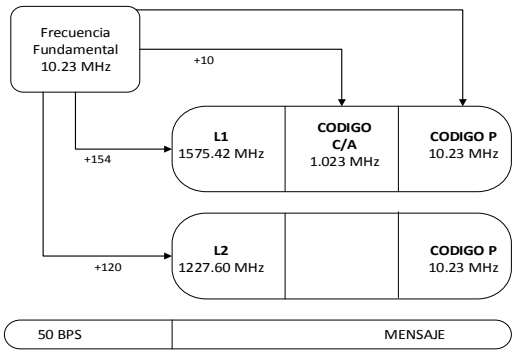

Figure 2. GPS signal structure. Based on [5]

The GPS system is used in the Smartphone of the victim so that the system can locate your position 24 hours of the day and identify areas of prohibition for aggressors.

4.2 GPRS

General Packet Radio Service (GPRS), created in the 80s for the data transmission by packet switching. With GPRS you can use services such as Wireless Application Protocol (WAP), short message service (SMS), multimedia messaging service (MMS), Internet and communication services such as email and the World Wide Web (WWW).

The format of a frame GPRS provides the following fields:

• GPRS protocol identifier

• Protocol identifier of the PDU (Protocol Data Unit)

• Post GPRS

GPRS protocol identifier is a numerical information, which aims to distinguish the different GPRS frames containing packets of frames containing information GSM. The protocol identifier of the PDUs encapsulated in GPRS frames need to address as soon as they are decapsulated, to the correct SAP (Service Access Point); also this information is numeric.

Because the messaging service GPRS is hired directly with a wireless carrier (Movistar), the identification and processing of these frames are made directly over the GSM / GPRS platform provider and the system should only be responsible for sending and receiving messages to and from mobile.

4.3 Bluetooth

Bluetooth is a radio system which operates in free frequency band of 2.4 GHz, this frequency band is available in the majority of the world. Bluetooth uses 79 radio frequency channels with a bandwidth of 1 MHz each and a maximum rate of 1 Msymbols / s. After each packet is sent on a particular frequency transmission, it changes to another one of the 79 frequencies. The typical operating range of Bluetooth is less than 10 m, but can achieve distances up to 100 m with the use of amplifiers. The Bluetooth communication is divided into several layers [6].
When the server or locators are doing a search device, send a Request signal equal to the figure below, the devices that are listening or waiting to analyze communication of the packet sent and if the access code corresponds to yours, answer the Request, otherwise just ignore it. This method achieve optimize system communications because they only will answer search of mobile devices that belong to our positioning system, ignoring all other Bluetooth devices.

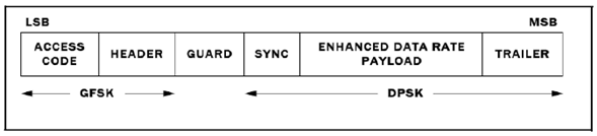

Figure 3. Bluetooth packet format. Based on [7]

To find Bluetooth devices that are within our reach, the terminal who performs the search must be in the state called by the Inquiry norm. This process consists in finding the access code assigned to the device in the 16 frequencies available for the inquiry. This process of discovery can be accomplished in two ways:

1. Normal mode: the length of device search is performed every 11.25 ms by default (Tw_inquiry_scan). This is done in a unique frequency hopping as defined in the XIR4-0 standard and which is determined on the basis of master clock device.

2. Interlaced: makes use of two exploration periods T_w_inquiry_scan. The value of this timer corresponds to 11.25 ms. The first period uses the

normal frequency jump, ie it is by XIR4-0 and the second is determined as [XIR4-0 + 16] mod32. In this situation, use of 32 dedicated frequencies are made, hence the need at least twice the browse window to make use of that mode

The option of running code Dedicated Access (DIAC) allows to configure mobile devices that only get associated with the beacon those configured devices with this code, thereby making the search much quicker because the beacon will discard the other Bluetooth devices as soon as they enter its own range and make pairing devices only registered in our system.

4.4 Raspberry PI Embedded System

Raspberry Pi is a computer board (SBC) inexpensive developed in the UK by the Raspberry Pi Foundation, with the objective of stimulating the teaching of computer science in schools.

The design of the Raspberry Pi includes a System-on-a-chip Broadcom BCM2835, which contains a central processor (CPU) ARM1176JZF-S 700 MHz (Turbo firmware includes ways for the user to make up to 1 GHz overclock without voiding the warranty), a graphics processor (GPU) VideoCore IV, and 512 MB. [8]

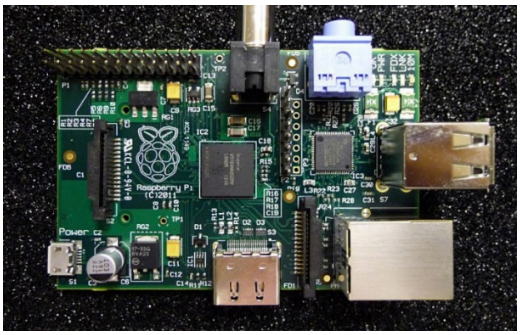

Figure 4. Raspberry Pi - B Model

5. EXPERIMENTAL SETUP

5.1 Communication

For the implementation of the beacon and communication with mobile locating devices it is necessary that the Raspberry Pi works with NMEA GPS, quadband GPRS, Bluetooth Class 1 and 802.11g Wi-Fi modules. The Raspberry Pi have the programming to initialize the search for indoor devices using Bluetooth, confirming the position with GPS, sending alerts to the victim through Bluetooth and GPRS, and transmission of information to the control center via GPRS and Wi-Fi .

Hardware of the implementation Faro

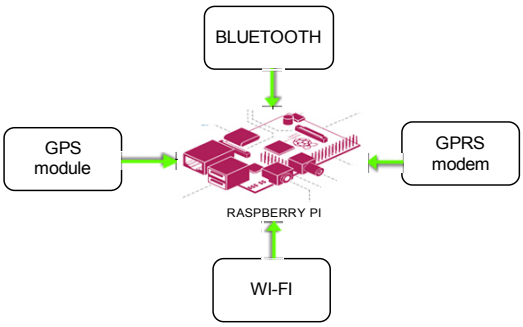

Figure 5. Hardware beacon on Raspberry Pi

Components chosen for implementation are:

Componente	Referencia
Embedded system	RASPBERRY-PI – BOARD ARM MODB-512M
GPS Module	GR89 GPS HOLUX MODULE
Bluetooth Module	30024-RN41 BLUETOOTH MODULE
GPRS Module	UC20-A - CELLULAR MODEM 3G
Wi-Fi Module	MRF24WB0MA/RM - MODULE WiFi / 802.11 TRANSCEIVER
RF Module	MRF49XA-IST TRANSCEIVER RF MODULE

Table 4. Hardware - beacon on Raspberry Pi

In the diagram below the implementation that is done for our own bracelet location is explained. As a central part is the microcontroller, who is in charge of making all instructions and apply math algorithms for data either supplied by the GPS or GSM module.

Hardware of the implementation Bracelet

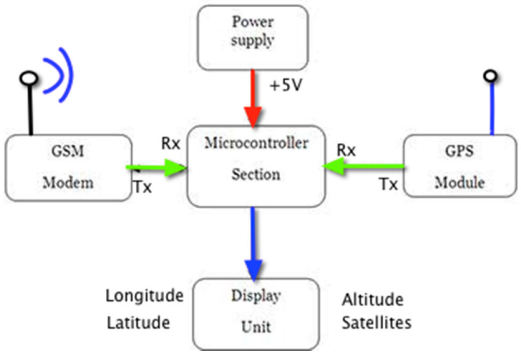

Figure 6. Hardware location bracelet

Discovery Devices flow chart

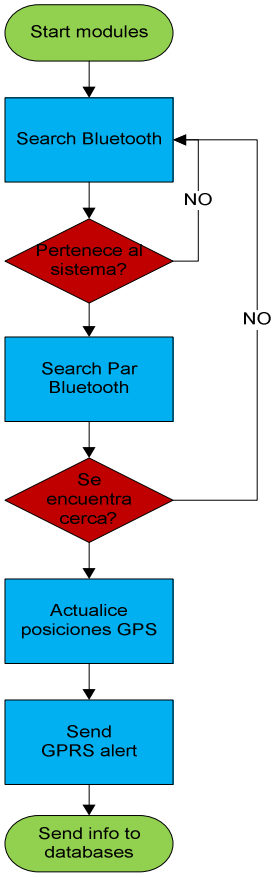

Figure 7. Discovery Devices

5.2 Coverage testing Bluetooth vs. WiFi

A performance test is defined as a technical investigation to determine or validate the speed, scalability and / or stability characteristics of a system under test [9]. Load tests are intended to simulate reality which shall be subject to the system (which is known as scenario) to analyze their performance to that situation.

Researchers at the University of Uruguay presented a methodology for performance testing [10] useful for load testing, but can be extended to other types of performance tests such as stress tests or tests peaks. Stress tests are focused on determining or validating performance characteristics of a system exposed to conditions beyond those anticipated for production, while testing peak refers to expose the system to sudden conditions increase in the burden for a short time.

The methodology consists of six stages: initial stage, requirements analysis, automation, Assembling the final infrastructure, execution and reporting, and final stage. The methodology focuses upon clearly identify the responsibilities of all parties involved and allows to analyze what activities are appropriate on-site with customers and which can be performed remotely. However, it can be used both by the development company to make their performance tests as any company that acquires a new system.

In this phase test range, speed and reliability of discovering communication protocols (Bluetooth and WiFi) to determine what the standard of indoor location were made.

1. Overview

The objective of the tests in this Annex is to evaluate the scope, speed and reliability of discovering Wi-Fi and Bluetooth devices installed on the "Faro" under normal system execution.

2. Test Phases

- Standard Installation and putting into service tests.
- Testing High Availability and Robustness..

The following table describes the tests run as part of this protocol.

EVIDENCE	TEST PHASE	TITLE TEST
MRF24WB0MA/RM - MODULO WiFi / 802.11 TRANSCEIV	Standard installation and putting into service tests.	• Connection Verification • Test the ignition cycle • Signal Quality • Speed of Discovery • Maximum distance of Recognition
	Testing High Availability and Robustness tez	• Availability of Hardware - Failure of electricity supply. • Availability of Hardware - Line Card Restart
30024-RN41 BLUETOOTH MODULE	Standard installation and putting into service tests.	• Connection Verification • Test the ignition cycle • Signal Quality • Speed of Discovery • Maximum distance of Recognition
	Testing High Availability and Robustness	• Availability of Hardware - Failure of electricity supply. • Availability of Hardware - Line Card Restart

Table 5. Bank of indoor standard tests.

3. Requirements and Assumptions

- The tests are performed at the "El Claustro" headquarters of the Catholic University of Colombia, in the area designated for 4 and 3 labs Electronics and courtyards.
- The communication modules Wi-Fi and Bluetooth must be pre-installed and configured to work on the Raspberry Pi.
- It should be written the scripts so that the Raspberry Pi automatically perform the search and discovery cycles.

EVIDENCE	TEST PHASE	TITLE TEST	AVERAGE TIME
Number of Attempts		5	
MRF24WB0MA/ RM - MODULO WiFi / 802.11 TRANSCEIV	Standard installation and putting into service tests.	Connection Verification	PASS
		On test cycle	26,5 s
30024-RN41 BLUETOOTH MODULE	Standard installation and putting into service tests.	Connection Verification	PASS
		On test cycle	33,7 s

Table 6. Connectivity tests

The following test was performed to determine the power of the beacon signal captured by the device when the victim is 15 meters away with line of sight.

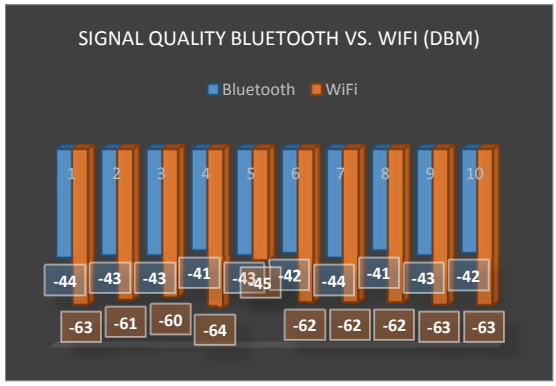

Figure 8. Signal Quality (Line of Sight)

To simulate a realistic scenario, a new test was made, this time with the devices to 20 m away without line of sight.

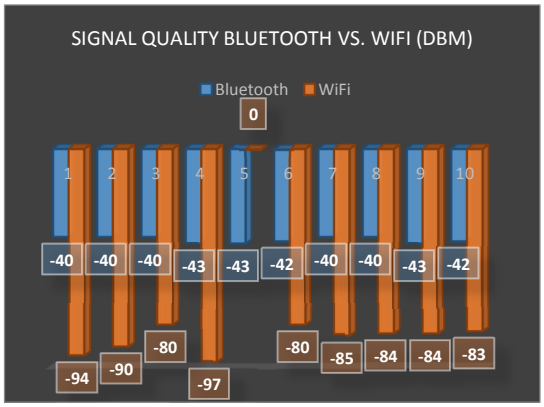

Figure 9. Signal Quality (without Line of Sight)

Maximum Recognition distance between Faro - Cellphone	
Description	Test to determine the maximum distance that the beacon identifies the MAC address of the WiFi device
Elements with which took place	Metro, 1 Cell Android, Raspberry Pi with WiFi module
Number of Attempts	6
Expected Results	Coverage of at least 15 meters
Results Obtained	Recognition distance about 25 meters, much higher than expected.
Observations	Distance / Obstacles / Results 5 meters / No / It is detected 10 meters / No / It is detected 10 meters / *Yes / It is detected 15 meters / *Yes / It is detected 20 meters / *Yes / It is detected 25 meters / *Yes / No detected
Conclusions	The maximum distance that the beacon reaches a WiFi device to detect and record its MAC is 20 meters in an enclosed with walls 30 cm thick between the beacon and the cellphone.

Table 7. Maximum Recognition distance between Faro - WiFi Cell

Maximum Recognition distance between Faro - Cellphone			
Description	Test to determine the maximum distance that the beacon identifies the MAC address of the WiFi device		
Elements	Metro, 1 Cell Android, Raspberry Pi with Bluetooth module		
Number of Attempts	8		
Expected Results	Coverage of at least 15 meters		
Results Obtained	Recognition distance is greater than 50 meters.		
Observations	Distance	Obstacles	Results
	5 meters	No	It is detected
	10 meters	No	It is detected
	10 meters	*Yes	It is detected
	15 meters	*Yes	It is detected
	20 meters	*Yes	It is detected
	30 meters	*Yes	It is detected
	40 meters	*Yes	It is detected
	50 meters	*Yes	It is detected
Conclusions	The beacon reaches a Bluetooth device to detect and record its MAC over 50 meters in an enclosed with walls 30 cm thick between the beacon and the cellphone.		

Table 8. Maximum Recognition distance between Faro - Bluetooth Cell

These initial tests were done in order to determine which wireless standards present on a cell phone, WiFi or Bluetooth, it is more appropriate to deploy indoor locating devices.

Table 7 shows that WiFi is a protocol that takes less time to be established, but this establishment will be given after reboot or be reset following a power failure, so it is presumed that only a few times during its cycle life will be performed.

Figures 8 and 9 show the power of the signal captured by the beacon, measured in dBm. First we see a scenario where the beacon and the cell of the victim have line of sight, ie, with no obstacles between them. The test results show that Bluetooth has to sign a power of 50% higher than WiFi, but both protocols work perfectly well.

In the second scenario, the devices are located further away and passages perpendicular to each other. What these tests show is that when there are walls in the signal path, Bluetooth Enhances reception power while WiFi decreases dramatically access to critical operating values. This is because the characteristics of the standards make WiFi being absorbed by obstacles such as walls, while Bluetooth bounces off them, increasing their scope.

Table 8 confirm the above said. When we vary the distance between the devices we note that WiFi has a maximum viewing distance of 20 meters, while Bluetooth exceeds 50 m radius, ensuring that devices may be recognized in a closed typical (building, shopping center space, hospital, etc.). It must be clarified that the beacon has a Bluetooth Class 1 device, with theoretical range of 100 meters.

It was concluded that because WiFi is a standard much more widespread today and its use is more prevalent among smartphone users, the rate of discovery and signal quality is much better using Bluetooth. In addition, the Bluetooth feature, which bounces off the concrete walls makes the distances and power levels be better in this standard against WiFi. Another reason for deciding on Bluetooth over WiFi is security, because WiFi is an open standard and easy to penetrate, while using dedicated access code (LIAC) of Bluetooth, all devices must be configured by hardware to be detected by the system.

The downside that has the Bluetooth protocol against WiFi is power consumption:

Battery life of the cellphone with running app	
Description	Test to determine the time it takes the application to consume the phone battery, being 100% of active time, no other activated functions.
Elements	1 Android Huawei cellphone
Number of Attempts	1
Expected Results	Battery consumption in approximately 18 hours.
Results Obtained	The battery ran out in about 24 hours showing that the program consumes only 6% of the battery
Conclusions	The battery consumption is not a barrier to the implementation of the platform.

Table 9. Battery life with the application

The DIAC dedicated access code guarantees that only devices configured with this code are bound by the system. Figures 10 and 11 show the

improvement in the discovery time when we use the DIAC code. Times are expressed in multiples of Length. A length is 1.28 second cycle, defined in the Bluetooth standard.

Analisis estadístico		
len	media	desviación
1	1,12	0,51
2	0,88	0,64
3	1,92	0,27
4	2	0
5	2	0
6	2	0
7	2	0
8	2	0
9	2	0
10	2	0

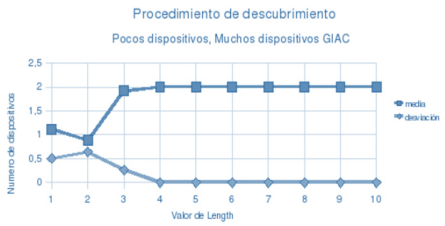

Figure 10. Discovery test Bluetooth normal Mode

Figure 11 shows that when we use the DIAC code for two mobile devices, the stabilization of the identified signal is reduced from 4 to 2 lenghts, that is, only 5.12 sec to 2.56 sec

Analisis estadístico		
len	media	desviación
1	1,88	0,32
2	2	0
3	2	0
4	2	0
5	2	0
6	2	0
7	2	0
8	2	0
9	2	0
10	2	0

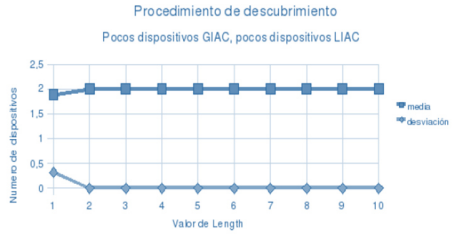

Figure 11. Discovery test Bluetooth interlaced Mode

5.3 Sustained Development Platform on Raspberry PI

Raspberry Pi is an embedded system, therefore, is a motherboard controlled by a microprocessor which already has USB ports, HDMI, LAN and GPIO communication, making virtually all communication modules that are used are plug and play and only need scripts to develop software to automate its operation.

Figure 12. Dongles Bluetooth and GPRS running on the Raspberry Pi

The interaction of the system components shown in Figure 13.

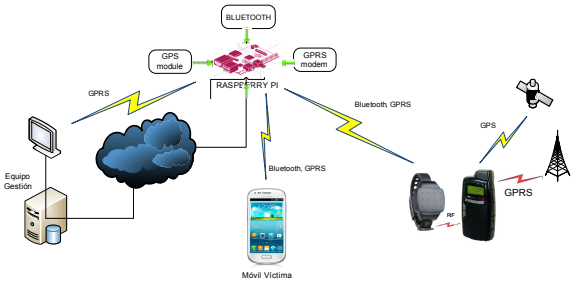

Figure 13. Interaction between system elements

Bluetooth and GPS testing devices based on the Raspberry and serves as a locator beacon module is carried out.

Identification of Bluetooth devices

Here can be viewed the search for Bluetooth devices from the Raspberry Pi

```
pi@raspberrypi ~ $ hcitool dev
Devices:
        hci0    00:15:83:15:A3:10
pi@raspberrypi ~ $ hcitool scan
Scanning ...
        7C:61:93:7F:C6:97       mcfunkybeard
pi@raspberrypi ~ $ sudo l2ping mcfunkybeard
Can't connect: Host is down
pi@raspberrypi ~ $ sudo l2ping 7C:61:93:7F:C6:97
Ping: 7C:61:93:7F:C6:97 from 00:15:83:15:A3:10 (data size 44) ...
44 bytes from 7C:61:93:7F:C6:97 id 0 time 7.86ms
44 bytes from 7C:61:93:7F:C6:97 id 1 time 90.50ms
44 bytes from 7C:61:93:7F:C6:97 id 2 time 122.78ms
44 bytes from 7C:61:93:7F:C6:97 id 3 time 202.83ms
44 bytes from 7C:61:93:7F:C6:97 id 4 time 134.87ms
44 bytes from 7C:61:93:7F:C6:97 id 5 time 137.73ms
^C6 sent, 6 received, 0% loss
pi@raspberrypi ~ $
```

Figure 14. Search for Bluetooth devices

Following the testing scheme presented in section 5.2, the test results Mobile recognition of the victim by the lighthouse is presented.

In a first series of tests a scenario in which the unit is active and the victim's cell phone is off but within the protected area is contemplated. Once the phone is turned on, we expect to recognize the beacon and if we do, also how long it takes.

Recognition 1 Between Beacon - Cell	
Description	Detection Test between the beacon and the victim's cell phone when the phone goes from off to on
Elements	1 Cell Android, Beacon implemented in the Raspberry Pi
Number of Attempts	10
Expected Results	Recognition in less than 1 minute

Results Obtained	Average time of 55 seconds
Observations	The mobile of the victim was identified in all attempts, always with time in the same range
Conclusions	Although the recommendation is always keep turned on mobile, given the case where the mobile is off and turn it on in the surveillance area, the system ensures that it will be found and associate in less than 1 minute.

Table 10. Test 1: Recognition between Faro - Cellphone

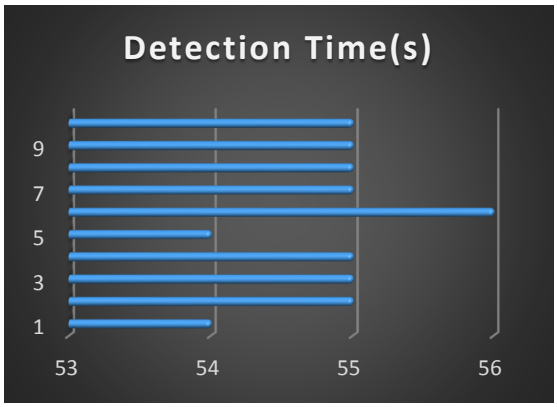

Figure 15. Bluetooth Signal Quality vs. WiFi (Line of sight)

This test showed that for scenario 1 (Mobile initially turned off), the system detects the mobile 100% of the time and in all cases takes less than 1 minute to do so.

A second detection test shows the expected normal operation scenario, ie working the beacon and the victim's cell phone is turned on to the protected area.

Figure 16. 'El Claustro' place plane

For these tests the beacon was located at a central point in the "El Claustro" headquarter of the Catholic University of Colombia, as in the 2nd floor of Block L on the IEEE room.

Given that the "El Claustro" headquarter has a complex architecture, labyrinth type L and M buildings, tests were divided into two sub-scenarios, one entering the parking lot of the career 16 and another entering the main access diagonal 47. Both scenarios show very different conditions because entering through the parking we have line of sight between the mobile and beacon, while when we walked through the diagonal access 47 we have a network of walls and hallways that represent an obstacle to direct communication between devices

Recognition 2 Between Beacon - Cell			
Description	Detection Test between the beacon and the victim's cell phone when the mobile moves toward the beacon		
Elements	1 Cell Android, Beacon implemented in the Raspberry Pi, metro		
Number of Attempts	6		
Expected Results	Detection at 40 meters		
Results Obtained	Higher detection distance of 40 meters		
Observations	Distance	Obstacles	Results
	40 meters	No	It is detected
	50 meters	No	Se detecta
	60 meters	No	Se detecta
	30 meters	*Yes	Se detecta
	40 meters	*Yes	Se detecta
	45 meters	*Yes	No detecta
Conclusions	Despite the complex architecture of the "El Claustro" headquarter, we guarantee that under the worst scenario will have a maximum distance of 40 meters recognition		

Table 11. Test 2: Recognition between Faro - Cellphone

Greeting delivery

Once the Bluetooth device has been identified and recognized as belonging the system the beacon sends a flat file containing a welcome message.

In Figure 17 can be seen an example of the message received by the mobile of the victim.

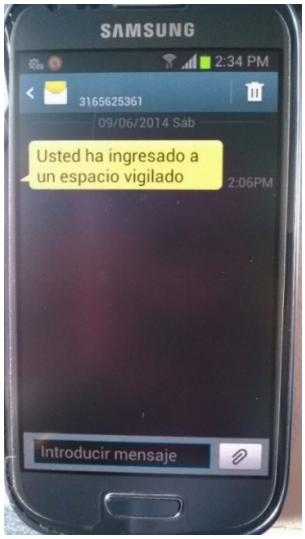

Figure 17. Welcome message to the system

GPS positioning

The device returns the GPS NMEA parameters, which, by the 'ImportString' command we import the exact location of the beacon: 4o63'39 " North, 74º06'88 " East

Raspberry Pi is a tool designed for free software and therefore exist on the network hundreds of lines of code that programmers available to all persons who want to use their code with the Raspberry Pi.

5.4 Implementation of Wireless Module in Control bracelet

Initially the components are deployed in a breadboard to make a series of preliminary tests and validate or not the design.

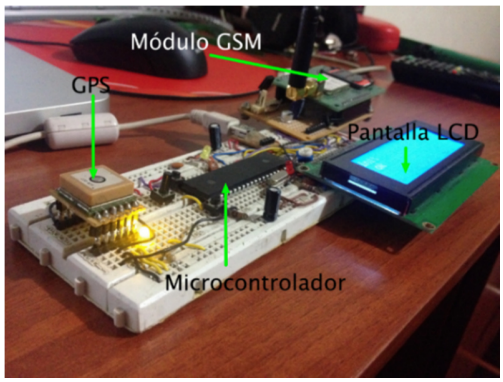

Figure 18. Implementation of modules for the bracelet

Similar to what happens with Raspberry way, Microchip has a community of developers who put their code to the service of those who want it. In the Microchip website we find the needed to put to work the NMEA GPS module: [11]

Here can be viewed the results of GPS location with the system running on the breadboard. It can be seen that the location given by the GPS module bracelet is the same as that provided by the GPS beacon in point 6.

Figure 19. GPS location results on the bracelet

Detection Bracelet tests

In this section tests are done to determine if the implemented system (Faro) is able to detect the RF band currently used by the authorities.
The module implemented in the beacon is the Microchip MRF49, operating in the bands 433 and 915 MHz, compatible with the bracelet ElmoTech used in government the Electronic Surveillance System.

Maximum Recognition Distance Beacon - Bracelet			
Description	Test to determine the maximum distance that the beacon identifies the bracelet ElmoTech		
Elements	Metro, Raspberry Pi with RF module, bracelet Elmotech		
Number of Attempts	7		
Expected Results	Scope at least 15 meters		
Results Obtained	Recognition distance is higher than 50 meters.		
Observations	Distancia	Obstáculos	Resultado
	5 meters	No	It is detected
	10 meters	No	It is detected
	15 meters	*Yes	It is detected
	20 meters	*Yes	It is detected
	25 meters	*Yes	It is detected
	30 meters	*Yes	It is not detected
	35 meters	*Yes	It is not detected
Conclusions	With state devices, the Beacon recognizes the bracelet 25 meters away.		

Table 12. Maximum Recognition distance between Faro – Bracelet

A second testbed considers our own bracelet and determine the maximum distance at which the moving of the victim is able to recognize.

Maximum Recognition Distance Cell - Bracelet			
Description	Test to determine the maximum distance that the victim's phone system identifies the bracelet.		
Elements	Metro, Cell Android, Bracelet of our system		
Number of Attempts	7		
Expected Results	Scope at least 15 meters		
Results Obtained	Recognition distance is higher than 50 meters.		
Observations	Distancia	Obstáculos	Resultado
	10 metros	Sin	Se detecta
	10 metros	*Con	Se detecta
	15 metros	*Con	Se detecta
	20 metros	*Con	Se detecta
	30 metros	*Con	Se detecta
	40 metros	*Con	Se detecta
	50 metros	*Con	No detecta
Conclusions	El móvil de la víctima corriendo con nuestra aplicación es capaz de detectar al brazalete diseñado por nosotros al menos 40 metros de distancia.		

Tabla 13. Maximum Recognition distance between Cellphone – Bracelet

Figure 20. Alert by proximity

The beacon on Raspberry designed system has proved effective both to locate and identify the victim's cell phone, the bracelet Elmotech currently used by the authorities and the new bracelet designed in this project.

The software application implemented on the mobile device of the victim is able to associate with the beacon, identify the proximity of the bracelet and receive SMS both welcome and warning messages.

The bracelet designed for this project has shown better range than the bracelet used by the authorities, with the added advantage that we have another extra location system such as Bluetooth is, not just RF bracelets as currently used by the judicial authorities.

5.5 Development - Application Management Team

Unified Modeling Language (UML) is a graphical language for visualizing, specifying and documenting each of the parts which comprises the development of software. UML provides a way to model conceptual things such as business processes and system functions as well as concrete things such as classes written in a particular language, database schemes, and reusable software components. [12], [13]

In the following diagram we can see the interaction between the beacon and mobile devices of the victim and the aggressor. Programming the Raspberry Pi must ensure that these steps are fulfilled.

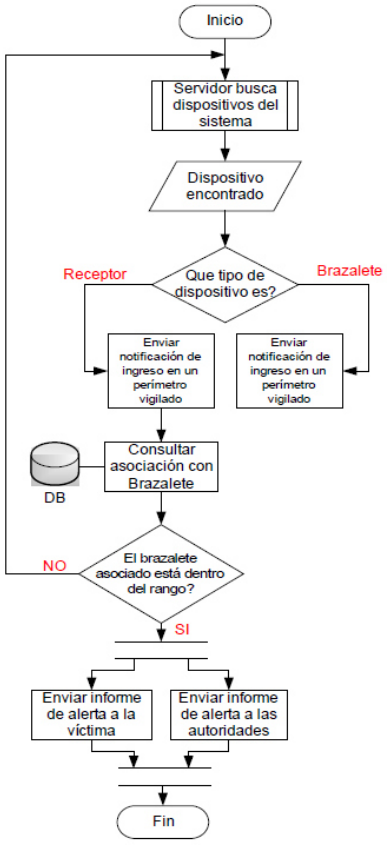

Figure 21. Flow chart between components

The network administrator must be previously registered in the system to authorized his username and password.

Figure 22. Team management home screen

6 RESULTS

6.4 Communication between the platform and Mobile Devices

In this chapter communication and data transmission between mobile devices and the management system is shown.

Figure 23. Location System Hardware

In Chapter 6 we can see the results of the testing of equipment individually or in pairs, beacon-bracelet, beacon-cell, cell-bracelet, but in this annex will see a little interaction with those management platform devices.

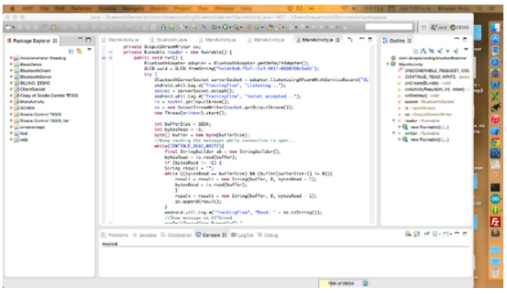

Figure 24. Bluetooth recognition notification to the platform

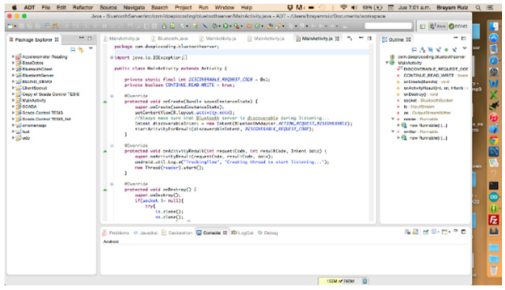

Figure 25. Notice of meeting to the platform

En Figure 25 can see the detailed information of GPS positioning the bracelet of the aggressor sends to the management team. You can program the frequency with which such information is sent to the central computer. This information is stored in the database of each device and serves as a record of all transactions made by the aggressor.

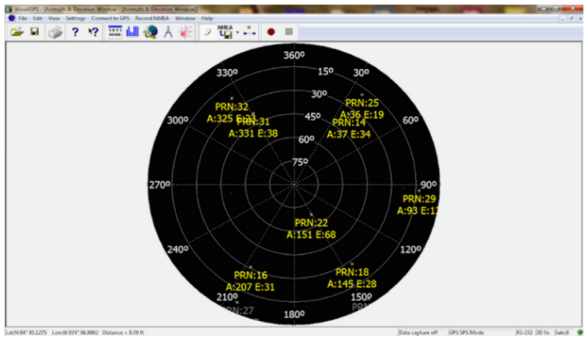

Figure 26. Aggressor satellite location

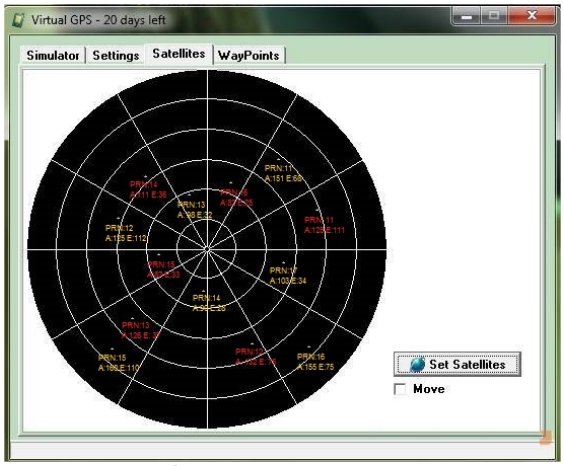

Figure 27. Satellite location victim-aggressor

Detailed information on the Figures 26 and 27 is easy to transmit and save, but not to interpret, therefore, the management team will have an application that can display more didactic way that information (Figure 28), note that it can view the current position of the aggressor and all positions that have been reported the bracelet.

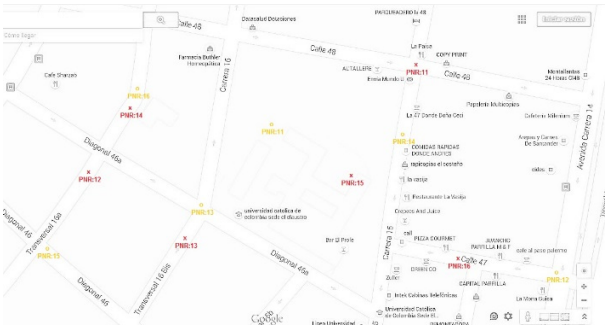

Figure 28. Location victim-aggressor on mobile

CONCLUSIONS

In the last decade the world has experienced unprecedented technological explosion. Technology has revolutionized the way of life of society and individual customs of each person, there are technological devices developed for different purposes, from the workplace to entertainment, through activities that were unthinkable a few decades ago using technology . The rise shown by mobile phone networks and the Internet make it important to use this technology to provide services that can help people improve their quality of life, facilitating their daily activities and provide security through TICs.

The goals set at the beginning of the project were successfully completed in its entirety since it has demonstrated the viability of producing a system of indoor positioning by bluetooth communication that complements the GPS systems used in the domestic penal system, it has verified the potential as far as communications are concerned the proposed system and its applicability in other fields and groups.

The more proved enriching acquired knowledge was related to understanding the suffering and anguish that must endure abuse-victims to see their movements limited by the possibility of a meeting with their batterers and existing drawbacks in the systems of monitoring and control convicts. It is due to these limitations of GPS systems that there are need to develop a system allowing victims of abuse and the prison authorities, have notion of the location of the system's stakeholders in closed spaces where GPS is inefficient.

The proposed positioning system is a viable indoor alternative that fill the void left by remote monitoring systems using GPS. Tests coverage, detection devices and speed of response show that the design and the technology used in the system are appropriate for ensure the victim of abuse, as the respective authorities, to be promptly informed if an encounter occurs with the batterer in the same monitored space.

The technological solution presented is simple and easy to implement both in the location and the receiver device that carries the victim. But as to the device that must wear the batterer, should make a complete study of economic and legislative viability to determine which option is the most feasible, whether to develop a completely new bracelet or adapt acquired system by the Colombian government.

BIBLIOGRAPHY

[1] World Health Organization. The World report on violence injury prevention, available on: http://www.who.int/violence_injury_prevention

[2] Alliance G Consultants & Center for Law Studies, Justice ans Society. Final Assessment Project operations of electronic surveillance systems, February 2012 report.

[3] Darío Fernando Cortez. Electronic platform for assistance to victims of gender violence indoor environments: Development of software tool based on a Linux operating system. Master's Thesis in Electronics, signal processing and communications. University of Seville, 2010, available at: http://www.dinel.us.es/grupos/aceti/docs/Documento3.pdf

[4] Castelán M. Ortiz, "Detection and Tracking Device Inspection and Maintenance (DIM) using the global positioning system (GPS) PEMEX networking product," University of the State of Hidalgo, Pachuca, 2007.

[5] JM Toloza, "Algorithms and techniques for real-time increased relative positional accuracy using standard GPS receivers," National University of La Plata, La Plata, 2012.

[6] "Implementation of a Bluetooth wireless network," Universidad del Valle, 2003, 2003.

[7] Zhou; Pollard, J.K. Position measurement using Bluetooth. Consumer Electronics, IEEE Transactions on Volume 52, Issue 2, May 2006 Page(s):555 – 558

[8] www.raspberrypi.org/

[9] J.D. Meier, Carlos Farre, Prashant Bansode, Scott Barber, Dennis Rea: Performance Testing Guidance for Web Applications. Microsoft Corporation, September 2007

[10] Toledo, Federico; Reina, Matías; Uvarow, Simon de; López, Horacio. Performance Testing Methodology.

Institute of Computer Science - Faculty of Engineering University of the Republic Montevideo, Uruguay, 2008

[11] GPSController.py. GiTHub.martinohanlon/pelmetcam, disponible en: https://github.com/martinohanlon/pelmetcam/blob/master/GPSController.py

[12] Arregui, Miguel. Tutorial de UML. Dept. Of Languages and Systems, University Jaume I. Castellón, 2004

[13] Peña, Lyda. Oriented Analysis and Design Using UML Object. Faculty of Engineering, Autonomous University of Colombia. Cali, 2004